

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-191302

(43)Date of publication of application : 21.07.1998

(51)Int.Cl.

H04N 7/167
H04H 1/00
H04L 9/08
H04L 9/14
H04N 5/91

(21)Application number : 08-351554

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 27.12.1996

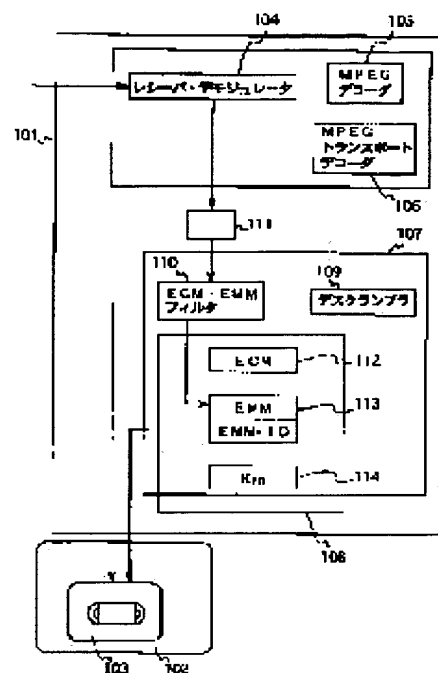
(72)Inventor : WATANABE KAZUHIRO

(54) DIGITAL SATELLITE BROADCAST RECEIVER

(57)Abstract:

PROBLEM TO BE SOLVED: To allow the user to be able to view a program after descramble even when a long time elapses after the program is recorded by storing separately intermediate key information that is separated from received data, other common key information and scramble program data together with intermediate key ID information.

SOLUTION: EMM(Entitlement Management Message) that is multiplexed on a satellite wave is transmitted. The EMM is extracted and ECM(Entitlement control Message) program data are filtered by an ECM.EMM filter 110 and stored in a program storage means 102. In the case of recording, an EMM-ID corresponding to the EMM is stored in a header area of an ECM program data storage area 113 in the recording. In the case of reproducing recording program data, an IC card 108 selects the EMM to which a matched EMM-ID is assigned from a list in the EMM storage area 113 with the clue of the received EMM-ID.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-191302

(43) 公開日 平成10年(1998) 7月21日

(51) Int.Cl. ⁶	識別記号	F I	
H 0 4 N 7/167		H 0 4 N 7/167	Z
H 0 4 H 1/00		H 0 4 H 1/00	H
			F
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A
9/14			6 4 1
審査請求 未請求 請求項の数22 O L (全 16 頁) 最終頁に続く			

(21) 出願番号 特願平8-351554

(22) 出願日 平成8年(1996)12月27日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 渡辺 一裕

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

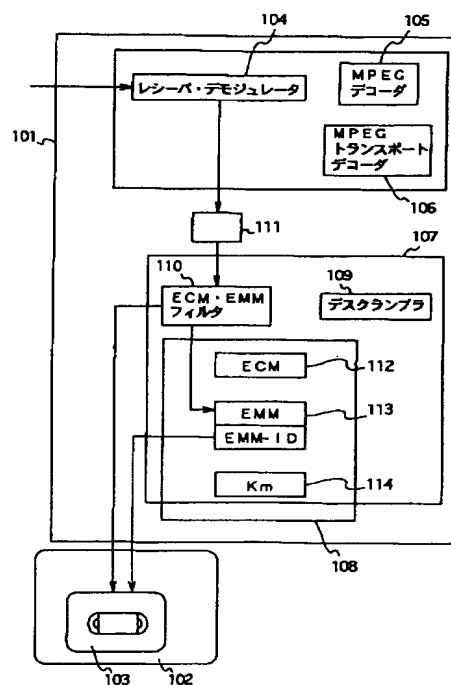
(74) 代理人 弁理士 池内 寛幸 (外2名)

(54) 【発明の名称】 デジタル衛星放送受信装置

(57) 【要約】

【課題】 共通鍵方式の3段階の鍵からデータがスクランブルされたデジタル衛星放送の番組記録およびその再生において、番組を記録した後、長期間が経過して中間鍵が更新された後でもスクランブルを解除することを可能とする。

【解決手段】 EMM、ECM番組データが多重化された衛星波を受信・復調するレシーバ・デモジュレータ104と、マスタ鍵を保持するマスタ鍵記憶手段114と、前記受信データをEMMとECM・番組データとに分離するECM・EMMフィルタ110と、前記EMMを追記記憶するEMM記憶手段113と、前記ECM・番組データ記録手段たる番組記録装置102と、前記ECM・番組データとそれに対応するEMMとの両者に両者を対応づけるEMM-IDをそれぞれに割り付けて記録するEMM-ID記録手段とを備え、番組データの再生にあたってEMM-IDを手掛かりに対応するEMMを選択して利用する。



【特許請求の範囲】

【請求項 1】 装置固有鍵と中間鍵と共通鍵からなる共通鍵暗号方式により番組データをスクランブルし、前記装置固有鍵により暗号化された中間鍵情報と前記中間鍵により暗号化された共通鍵情報と前記共通鍵により暗号化されたスクランブル番組データとを衛星波に多重化して配信するデジタル放送システムに利用されるデジタル衛星放送受信装置において、前記多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を保持する装置固有鍵記憶手段と、前記受信したデータを中間鍵情報と共通鍵情報・スクランブル番組データとに分離する中間鍵情報フィルタと、前記分離した中間鍵情報を記憶する中間鍵情報記憶手段と、前記分離された共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データとそれに対応する中間鍵情報との両者に両者を対応づける中間鍵 I D 情報をそれぞれに割り付けて記録する中間鍵 I D 情報記録手段とを備えたことを特徴とするデジタル衛星放送受信装置。

【請求項 2】 装置固有鍵と中間鍵と共通鍵からなる共通鍵暗号方式により番組データをスクランブルし、前記中間鍵により暗号化された共通鍵情報と前記共通鍵により暗号化されたスクランブル番組データとを衛星波に多重化して配信するデジタル放送システムに利用されるデジタル衛星放送受信装置において、前記装置固有鍵により暗号化された中間鍵情報を受信する手段と、前記多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を記憶する装置固有鍵記憶手段と、前記受信した中間鍵情報を記憶する中間鍵情報記憶手段と、前記受信した共通鍵情報とスクランブル番組データとを記録する共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データとそれに対応する中間鍵情報との両者に両者を対応づける中間鍵 I D 情報をそれぞれに割り付けて記録する中間鍵 I D 情報記録手段とを備えたことを特徴とするデジタル衛星放送受信装置。

【請求項 3】 前記中間鍵情報記憶手段において、中間鍵情報および中間鍵 I D 情報の書き込みにあたり現存データに上書きせず追記保存する請求項 1 または 2 に記載のデジタル衛星放送受信装置。

【請求項 4】 前記記録されている共通鍵情報・スクランブル番組データと中間鍵 I D 情報を読み出す記録データ読み出し手段と、前記読み出された中間鍵 I D 情報と一致する中間鍵 I D 情報に対応付けられて記憶されている中間鍵情報を選択する中間鍵情報選択手段と、前記読み出された共通鍵情報とスクランブル番組データを分離する共通鍵情報フィルタと、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵に

よって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えた請求項 1 または 2 に記載のデジタル衛星放送受信装置。

【請求項 5】 前記中間鍵情報記憶手段において、前記記録する装置が持つ装置固有鍵により復号される中間鍵情報のほか、他の装置に与えられた装置固有鍵により復号される中間鍵情報も併せて記憶する請求項 1 または 2 に記載のデジタル衛星放送受信装置。

【請求項 6】 装置が装置固有の装置 I D 情報を持ち、前記中間鍵情報記憶手段において、前記記憶する中間鍵情報に対応する装置固有鍵を持つ装置の装置 I D 情報も併せて記憶する請求項 5 に記載のデジタル衛星放送受信装置。

【請求項 7】 自らの装置 I D 情報およびあらかじめ相互利用が設定されている他の装置の装置 I D 情報を記憶する手段と、装置が前記中間鍵情報を受信した場合に伴っている装置 I D 情報と前記装置内に記憶している装置 I D 情報とを比較する装置 I D 比較手段と、前記装置 I D 比較手段において一致するものがあれば前記中間鍵情報記憶領域に前記中間鍵情報とその対応する装置 I D 情報とを合わせて記憶する手段とを備えた請求項 6 に記載のデジタル衛星放送受信装置。

【請求項 8】 前記装置 I D 情報と中間鍵 I D 情報を手掛かりとして再生・視聴する番組データに対応する中間鍵情報を記憶されている中間鍵 I D 情報の中から選択する中間鍵情報選択手段と、前記共通鍵情報とスクランブル番組データとを分離する共通鍵情報・スクランブル番組データ分離手段と、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えた請求項 6 または 7 に記載のデジタル衛星放送受信装置。

【請求項 9】 装置固有鍵と中間鍵と共通鍵からなる共通鍵暗号方式により番組データをスクランブルし、前記装置固有鍵により暗号化された中間鍵情報と前記中間鍵により暗号化された共通鍵情報と前記共通鍵により暗号化されたスクランブル番組データとを衛星波に多重化して配信するデジタル放送システムに利用されるデジタル衛星放送受信装置において、前記多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を記憶する装置固有鍵記憶手段と、前記受信したデータを中間鍵情報と共通鍵情報・スクランブル番組データとに分離する中間鍵情報フィルタと、前記分離した中間鍵情報を記憶する中間鍵情報記憶手段と、前記分離された共通鍵情報・スクランブル番組データを記録する

共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データ記録手段に対して前記記憶されている中間鍵情報を伝達し、共通鍵情報・スクランブル番組データとともに記録する手段とを備えたことを特徴とするデジタル衛星放送受信装置。

【請求項 10】 前記記録されている共通鍵情報・スクランブル番組データと中間鍵情報を読み出す記録データ読み出し手段と、前記読み出された共通鍵情報とスクランブル番組データを分離する共通鍵情報フィルタと、前記装置固有鍵と前記中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えた請求項 9 に記載のデジタル衛星放送受信装置。

【請求項 11】 前記中間鍵情報記憶手段において、前記記憶する装置が持つ装置固有鍵により復号される中間鍵情報のほか、他の装置に与えられた装置固有鍵により復号される中間鍵情報も併せて記憶する請求項 9 または 10 に記載のデジタル衛星放送受信装置。

【請求項 12】 装置が装置固有の装置 ID 情報を持ち、前記中間鍵情報記憶手段において、前記記憶する中間鍵情報に対応する装置固有鍵を持つ装置の装置 ID 情報も併せて記憶する請求項 11 に記載のデジタル衛星放送受信装置。

【請求項 13】 自らの装置 ID 情報およびあらかじめ相互利用が設定されている他の装置の装置 ID 情報を記憶する手段と、装置が前記中間鍵情報を受信した場合に伴っている装置 ID 情報と前記装置内に記憶している装置 ID 情報とを比較する装置 ID 情報比較手段と、前記装置 ID 情報比較手段において一致するものがあれば前記中間鍵情報記憶領域に前記中間鍵情報とその対応する装置 ID 情報とを合わせて記憶する手段とを備えた請求項 12 に記載のデジタル衛星放送受信装置。

【請求項 14】 前記装置 ID 情報を手掛かりとして再生・視聴する番組データに対応する中間鍵情報を前記記憶されている中間鍵情報の中から選択する中間鍵情報選択手段と、前記共通鍵情報とスクランブル番組データを分離する共通鍵情報・スクランブル番組データ分離手段と、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えた請求項 12 または 13 に記載のデジタル衛星放送受信装置。

【請求項 15】 前記中間鍵情報および対応する中間鍵

ID 情報の記憶領域が、前記装置固有鍵の記憶領域がある記憶媒体と同じ記憶媒体内に設けられている請求項 1 または 2 に記載のデジタル衛星放送受信装置。

【請求項 16】 前記記憶媒体が IC カードである請求項 15 に記載のデジタル衛星放送受信装置。

【請求項 17】 前記中間鍵情報記憶領域が複数の記憶媒体にあり、1 つは前記装置固有鍵の記憶領域がある記憶媒体の中に設けられ、他方は前記装置固有鍵の記憶領域がある記憶媒体とは別の記憶媒体に設けられた請求項 1 または 2 に記載のデジタル衛星放送受信装置。

【請求項 18】 前記他方の記憶媒体がメモリカードである請求項 17 に記載のデジタル衛星放送受信装置。

【請求項 19】 前記共通鍵情報・スクランブル番組データの記録領域が装置に内蔵または外付けで接続された記録媒体にある請求項 1, 2, 9, 10 のいずれか 1 項に記載のデジタル衛星放送受信装置。

【請求項 20】 前記記録媒体が磁気ディスク、内蔵メモリ、またはメモリカードである請求項 19 に記載のデジタル衛星放送受信装置。

【請求項 21】 前記共通鍵情報・スクランブル番組データの記録領域が可搬性を持った記録媒体にある請求項 1, 2, 9, 10 のいずれか 1 項に記載のデジタル衛星放送受信装置。

【請求項 22】 前記記録媒体が磁気テープ、光磁気ディスク、DVD、CD-R、フォト CD またはメモリカードである請求項 21 に記載のデジタル衛星放送受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデジタル衛星放送等のデジタル放送の受信装置に関する。

【0002】

【従来の技術】近年、衛星を利用したデジタル放送が広がりつつある。デジタル衛星放送では、CATVとは違って番組データは衛星から地上へ向けて放射され、パラボラアンテナなどの電波受信装置があれば誰でも受信できるものであるため、視聴契約など正当に視聴する権利のない者の受信を排除する目的でデータにスクランブルをかけるのが一般的である。また多チャンネル化に伴って複数の放送番組が多重化されてデータが送信されるため、その視聴者が契約した番組のみを視聴させるためにもデータのスクランブルは必要となっている。ここで、スクランブルのセキュリティを高め、視聴者別、番組別の視聴権利の管理のため、共通鍵暗号方式を利用した 3 重鍵構造の限定受信方式が採用されている。

【0003】図 9 および図 10 は 3 重鍵構造の限定受信方式を採用したデジタル放送受信装置およびこれに接続される番組記憶装置の構成を示すものである。図 9 が番組の録画のときのデータの流れ、図 10 が再生のときのデータの流れを示している。暗号鍵として、マスタ鍵

5

(K_m)、中間鍵たるワーク鍵(K_w)、番組データのデスクランブルを行なう共通鍵たるスクランブル鍵(K_s)の3重構造を採用する。ここで前記ワーク鍵K_wをマスタ鍵K_mで暗号化した情報を限定受信個別管理情報(E_{MM}:Entitlement Management Message)とし、前記スクランブル鍵をワーク鍵で暗号化したものを限定受信共通情報(E_{CM}:Entitlement Control Message)とする。

【0004】図9および図10において、901はデジタル放送受信装置いわゆるセットトップボックス、902はデジタルVTRなどの番組記憶装置、903は磁気テープなどの記憶媒体、904はチューナと復調器から構成される衛星波を受信・復調するレシーバ・デモジュレータ、905はMPEGデコーダ、906はMPEGトランスポートデコーダ、907は限定受信を行うためのセキュリティモジュール、908はセキュリティモジュール内で限定受信管理を行うICカード、909はスクランブルを解除するためのデスクランブラ、910はスクランブルを解除するために必要な鍵を含んだ情報である前記限定受信共通情報(E_{CM})および限定受信個別管理情報(E_{MM})をMPEGトランスポートストリームから選択するためのE_{CM}・E_{MM}フィルタ、911はMPEGトランスポートストリーム入力切回路、912はICカード908内に格納されているE_{CM}、913はICカード908内に格納されているE_{MM}である。

【0005】3重鍵構造の限定受信方式では、MPEG方式でデジタル圧縮された画像・音声情報をスクランブル鍵K_sにて暗号化する。秘匿性を高めるためスクランブル鍵K_sは1秒程度毎に更新される。スクランブル鍵K_sはワーク鍵K_wにて暗号化され限定受信共通情報E_{CM}として、画像・音声情報のデータにMPEGトランスポート多重化されて伝送される。ワーク鍵K_wは、各デジタル放送受信装置に固有な鍵であるマスタ鍵K_mにて暗号化され限定受信個別管理情報E_{MM}として、これもワーク鍵K_wと同様にMPEGトランスポート多重化されて伝送される。なおマスタ鍵K_mは各デジタル放送受信装置で異なるため、E_{MM}もそれぞれ異なり、他のデジタル放送受信装置に対応するE_{MM}を使用することはできない。

【0006】デジタル放送番組をデジタル情報のままデジタルVTR等を用いて記録できれば、デジタル放送の高画質を再生時にも活かすことが可能となる。しかし、映画等の著作権の保護を考慮すると、再生時にも限定受信機能と同じ機能が働くことが望ましい。すなわちスクランブルがかかったままの状態デジタルVTR等に記録し、視聴権利を持つデジタル放送受信装置でのみスクランブル解除を可能とする。図9はこのように目的のために構成したデジタル放送受信装置の構成を示すものである。図9では、番組の放送されている

6

時間内のデータをそのまま記録するように構成されており、番組記録装置902に対してE_{CM}および番組のMPEGデータを伝送し、記録媒体903に記録する。E_{MM}913は長周期で更新されるため一般にはICカード908内に格納されている。

【0007】

【発明が解決しようとする課題】しかしながら、従来のデジタル衛星放送受信における暗号管理方式および放送番組記録方式においては、番組を記録媒体903に記録した後、しばらくは問題なく再生可能であるが、E_{MM}913が更新された場合、記録された番組に対するワーク鍵K_wが失われることになり、スクランブルを解除することが不可能となる。番組データのスクランブルセキュリティを保つため、前記のように従来例ではスクランブル鍵K_sは1秒ごとという短周期で更新し、ワーク鍵K_wも1か月程度で更新される。つまり視聴者に送信されるE_{CM}およびE_{MM}が前記周期で更新される。更新後のE_{MM}をマスタ鍵K_mで復号して得られるワーク鍵K_wは、前記放送番組データとともに記録されているE_{CM}には対応していないものであり、前記ワーク鍵K_wで前記記録されているE_{CM}を復号して得られるスクランブル鍵K_sは記録番組データのスクランブル鍵ではない。よって記録した番組データの再生ができなくなってしまうという問題があった。

【0008】また、複数世帯が同居など視聴者の都合により複数の受信契約があり、複数の受信装置を同時に使用する権利が設定されている場合があるが、記録された番組を他のデジタル放送受信装置を用いて再生する場合においてもワーク鍵K_wもともと相違し、または更新されることにより失われることがあり、スクランブルを解除することが不可能となる可能性があった。

【0009】本発明は、番組を記録した後、長期間が経過してもスクランブルを解除し視聴することを可能とする方法および、記録に用いたデジタル放送受信装置とは異なる第2のデジタル放送受信装置で再生した場合でも同様にスクランブルを解除し視聴することを可能とする制御ができるデジタル衛星放送受信装置を提供することを目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するために本発明に係るデジタル衛星放送受信装置は、多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を保持する装置固有鍵記憶手段と、前記受信したデータを中間鍵情報と共通鍵情報・スクランブル番組データとに分離する中間鍵情報フィルタと、前記分離した中間鍵情報を追記記憶する中間鍵情報記憶手段と、前記分離された共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データとそれに対応する中間鍵情報との両者に両者を対応づける中間鍵ID情報をそれぞれに割り付けて記録す

る中間鍵 I D 情報記録手段とを備える。

【0011】かかる構成により、本発明に係るデジタル衛星放送受信装置は、多重化されて送られてくるデータから中間鍵情報をその他の共通鍵情報・スクランブル番組データから分離した後に中間鍵 I D 情報とともに別途記憶させておくことができ、後日の利用に供することができる。

【0012】また上記目的を達成するために本発明に係るデジタル衛星放送受信装置は、装置固有鍵により暗号化された中間鍵情報を受信する手段と、前記多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を保持する装置固有鍵記憶手段と、前記受信した中間鍵情報を追記記憶する中間鍵情報記憶手段と、前記受信した共通鍵情報とスクランブル番組データとを記録する共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データとそれに対応する中間鍵情報との両者に両者を対応づける中間鍵 I D 情報をそれぞれに割り付けて記録する中間鍵 I D 情報記録手段とを備える。

【0013】かかる構成により本発明に係るデジタル衛星放送受信装置は、中間鍵情報を電話回線などにより受信した場合に受信装置内に中間鍵 I D 情報とともに記憶させておくことができ、後日、前記記録されている中間鍵情報の中から、対応付けられている中間鍵 I D 情報を手掛かりに記録データに対応する中間鍵を特定して利用することができる。

【0014】さらに前記デジタル衛星放送受信装置は、前記中間鍵情報記録手段において、前記記録された中間鍵情報は上書きせずに前記中間鍵 I D 情報とともに来歴記録として保存することが好ましい。

【0015】かかる構成により、記録番組データに対応する中間鍵情報が失われることなく、後日記録番組データの視聴にあたって、前記記憶されている中間鍵情報の中から中間鍵 I D 情報を基に記録番組データに対応する中間鍵を特定することができる。

【0016】また上記目的を達成するために本発明に係るデジタル衛星放送受信装置は、前記記録されている共通鍵情報・スクランブル番組データと中間鍵 I D 情報を読み出す記録データ読み出し手段と、前記読み出された中間鍵 I D 情報と一致する中間鍵 I D 情報に対応付けられて記憶されている中間鍵情報を選択する中間鍵情報選択手段と、前記読み出された共通鍵情報とスクランブル番組データを分離する共通鍵情報フィルタと、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備える。

【0017】かかる構成により、後日の記録番組データの視聴にあたって、中間鍵 I D 情報を手掛かりに、再生・視聴する番組データに対応する中間鍵情報を記録されている中間鍵情報の中から選択することができ、その中間鍵から得た共通鍵を用いて、記録番組データのスクランブルを解除して再生・視聴することができる。

【0018】次に前記デジタル衛星放送受信装置は、前記中間鍵情報記憶手段において、前記記録する装置が持つ装置固有鍵により復号される中間鍵情報のほか、他の装置に与えられた装置固有鍵により復号される中間鍵情報も併せて記憶することが好ましい。

【0019】かかる手段により、視聴権利を持つ複数の装置において、データを相互に再生、視聴するために必要な中間鍵を相互に持つことができる。

【0020】次に前記デジタル衛星放送受信装置は、装置固有の装置 I D 情報を持ち、前記中間鍵情報記憶手段において、前記記憶する中間鍵情報に対応する装置固有鍵を持つ装置の装置 I D 情報も併せて記憶することが好ましい。

【0021】かかる手段により、後日の記録番組データの視聴にあたって、装置 I D 情報および中間鍵 I D 情報を手掛かりに、再生・視聴する装置に対応し、かつ再生・視聴する番組データに対応する中間鍵情報を記録されている中間鍵情報の中から選択することができる。

【0022】次に前記デジタル衛星放送受信装置は、自らの装置 I D 情報およびあらかじめ相互利用が設定されている他の装置の装置 I D 情報を保持する手段と、装置が前記中間鍵情報を受信した場合に伴っている装置 I D 情報と前記装置内に保持している装置 I D 情報とを比較する装置 I D 比較手段と、前記装置 I D 比較手段において一致するものがあれば前記中間鍵情報記憶領域に前記中間鍵情報とその対応する装置 I D 情報とを合わせて記憶する手段とを備えることが好ましい。

【0023】かかる構成により、あらかじめ設定されている他の装置を利用した後日での再生に備え、保持しておくべき中間鍵情報を判別し、中間鍵 I D 情報に対応付けて保持しておくことができる。

【0024】次に前記デジタル衛星放送受信装置は、装置 I D 情報と中間鍵 I D 情報を手掛かりとして再生・視聴するデータに対応する中間鍵情報を記憶されている中間鍵 I D 情報の中から選択する中間鍵情報選択手段と、前記共通鍵情報とスクランブル番組データを分離する共通鍵情報・スクランブル番組データ分離手段と、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えることが好ましい。

【0025】かかる手段により、後日の記録番組データの視聴にあたって、装置ID情報および中間鍵ID情報を手掛かりに、再生・視聴する装置に対応し、かつ再生・視聴する番組データに対応する中間鍵情報を記録されている中間鍵情報の中から選択することができ、その中間鍵から得た共通鍵を用いて、記録番組データのスクランブルを解除して再生・視聴することができる。

【0026】上記目的を達成するために本発明に係るデジタル衛星放送受信装置は、多重化された衛星波を受信・復調するレシーバ・デモジュレータと、前記装置固有鍵を保持する装置固有鍵記憶手段と、前記受信したデータを中間鍵情報と共通鍵情報・スクランブル番組データとに分離する中間鍵情報フィルタと、前記分離した中間鍵情報を記憶する中間鍵情報記録手段と、前記分離された共通鍵情報・スクランブル番組データを記録する共通鍵情報・スクランブル番組データ記録手段と、前記共通鍵情報・スクランブル番組データ記録手段に対して前記記憶されている中間鍵情報を伝達し、共通鍵情報・スクランブル番組データとともに記録する中間鍵情報記録手段とを備える。

【0027】かかる構成により、本発明に係るデジタル衛星放送受信装置は、多重化されて送られてくるデータから中間鍵情報をその他の共通鍵情報・スクランブル番組データから分離して有効な中間鍵情報を記憶し、番組データの記録時点で中間鍵情報を共通鍵情報・スクランブル番組データ記録手段に伝達して番組データと併せて記録することができる。

【0028】次に前記デジタル衛星放送受信装置は、前記記録されている共通鍵情報・スクランブル番組データと中間鍵情報を読み出す記録データ読み出し手段と、前記読み出された共通鍵情報とスクランブル番組データを分離する共通鍵情報フィルタと、前記装置固有鍵と前記中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えることが好ましい。

【0029】かかる構成により、中間鍵情報記憶手段により記憶されている中間鍵情報が更新された後であっても、スクランブル番組データと対応する中間鍵情報を利用することができ、番組データを再生することができる。

【0030】次に前記デジタル衛星放送受信装置は、前記中間鍵情報記憶手段において、前記記録する装置が持つ装置固有鍵により復号される中間鍵情報のほか、他の装置に与えられた装置固有鍵により復号される中間鍵情報も併せて記憶することが好ましい。

【0031】かかる手段により、視聴権利を持つ複数の

装置において、データを相互に再生・視聴するために必要な中間鍵を相互に持つことができる。

【0032】次に前記デジタル衛星放送受信装置は、装置固有の装置ID情報を持ち、前記中間鍵情報記憶手段において、前記記憶する中間鍵情報に対応する装置固有鍵を持つ装置の装置ID情報も併せて記憶することが好ましい。

【0033】かかる手段により、後日の記録番組データの視聴にあたって、装置ID情報を手掛かりとして、再生・視聴する装置に対応し、かつ再生・視聴する番組データに対応する中間鍵情報を記録されている中間鍵情報の中から選択することができる。

【0034】次に前記デジタル衛星放送受信装置は、自らの装置ID情報およびあらかじめ相互利用が設定されている他の装置の装置ID情報を保持する手段と、前記装置が前記中間鍵情報を受信した場合に伴っている装置ID情報と前記装置内に保持している装置ID情報とを比較する装置ID情報比較手段と、前記装置ID情報比較手段において一致するものがあれば前記中間鍵情報記憶領域に前記中間鍵情報とその対応する装置ID情報とを合わせて記憶する手段とを備えることが好ましい。

【0035】かかる構成により、あらかじめ設定されている他の装置を利用した後日の再生に備え、保持しておくべき中間鍵情報を判別して保持しておくことができる。

【0036】次に前記デジタル衛星放送受信装置は、装置ID情報を手掛かりとして再生・視聴するデータに対応する中間鍵情報を記憶されている中間鍵情報の中から選択する中間鍵情報選択手段と、前記共通鍵情報とスクランブル番組データを分離する共通鍵情報・スクランブル番組データ分離手段と、前記装置固有鍵と前記選択した中間鍵情報と前記分離された共通鍵情報とから共通鍵を得る共通鍵復号手段と、前記分離されたスクランブル番組データを前記共通鍵復号手段で得られた共通鍵によって復号化するスクランブル番組データ復号化手段と、前記スクランブル番組データ復号化手段によって復号されたデータを視聴するための復号データ視聴手段とを備えることが好ましい。

【0037】かかる手段により、後日の記録番組データの視聴にあたって、装置ID情報を手掛かりに、再生・視聴する装置に対応し、かつ再生・視聴する番組データに対応する中間鍵情報を記録されている中間鍵情報の中から選択することができ、その中間鍵から得た共通鍵を用いて、記録番組データのスクランブルを解除して再生・視聴することができる。

【0038】次に前記デジタル衛星放送受信装置において、前記中間鍵情報および対応する中間鍵ID情報の記憶領域が、前記装置固有鍵を記憶している記憶領域がある記憶媒体と同じ記憶媒体内に設けられることが好ましい。

【0039】さらに前記記憶媒体がICカード記憶媒体であることが好ましい。

【0040】かかる構成により、マスタ鍵を持つ記憶媒体が使用されているデジタル衛星放送受信装置に中間鍵情報および中間鍵ID情報が確実に記憶され、前記記憶媒体を他の装置に挿入してその装置をデジタル衛星放送受信装置として使用する場合などにおいても中間鍵情報が失われることなく、記録番組データの再生・視聴ができる。

【0041】次に前記デジタル衛星放送受信装置において、前記中間鍵情報記憶領域が複数の記憶媒体にあり、1つは前記装置固有鍵の記憶領域がある記憶媒体の中に設けられ、他方は前記装置固有鍵の記憶領域がある記憶媒体とは別の記憶媒体に設けられることが好ましい。

【0042】さらに前記記憶媒体がメモリカードであることが好ましい。

【0043】かかる構成により、現行の中間鍵情報をマスタ鍵の記憶領域がある記憶媒体と同じ記憶媒体に記憶でき、かつ記録した番組データに対応する中間鍵情報および中間鍵ID情報をマスタ鍵のある記憶媒体とは別の記憶媒体に記憶させることができ、かかる中間鍵情報および中間鍵ID情報のみを分離することができる。

【0044】次に前記デジタル衛星放送受信装置において、前記共通鍵情報・スクランブル番組データの記憶領域が装置に内蔵または外付けで接続された記憶媒体にあることが好ましい。

【0045】さらに前記記憶媒体が磁気ディスク、内蔵メモリ、またはメモリカードであることが好ましい。

【0046】かかる構成により、記録データの後日の再生・視聴にあたり、衛星デジタル受信装置内部で高速に記録データにアクセスできる。

【0047】また前記デジタル衛星放送受信装置において、前記共通鍵情報・スクランブル番組データの記憶領域が可搬性を持った記憶媒体にあることが好ましい。

【0048】さらに前記記憶媒体が磁気テープ、光磁気ディスク、DVD（デジタルビデオディスク）、CD-R（追記型CD）、フォトCDまたはメモリカードであることが好ましい。

【0049】かかる構成により、記録した放送番組データを可搬性あるものとでき、大量データの記録保存、他の衛星デジタル受信装置での利用に供することができる。

【0050】

【発明の実施の形態】以下、本発明の実施形態について、図1および図8を用いて説明する。

【0051】（実施の形態1）本実施形態1は、デジタル衛星放送の番組を記録した後、長期間が経過してもスクランブルを解除し視聴することを可能とするデジタル衛星放送受信装置である。本実施形態1は共通鍵暗号方式を利用した3重鍵構造の限定受信方式による衛星放送

システムを前提としており、暗号鍵は、マスタ鍵Km、中間鍵たるワーク鍵Kw、番組データのデスクランブルを行なう共通鍵たるスクランブル鍵Ksの3重の鍵からなり、ワーク鍵Kwをマスタ鍵Kmで暗号化した中間鍵情報を限定受信個別管理情報EMM（Entitlement Management Message）とし、前記スクランブル鍵をワーク鍵で暗号化した共通鍵情報を限定受信共通情報ECM（Entitlement Control Message）とする。以下、EMMの記憶、衛星デジタル番組データおよびECMの記録、記憶データの再生・視聴の3つの段階に分けて説明する。

【0052】まず、EMMの記憶について示す。図1は本発明の第1の実施形態におけるデジタル衛星放送受信装置の構成図である。図1において、101はデジタル放送受信装置いわゆるセットトップボックス、102はデジタルVTRなどの番組記憶装置、103は磁気テープなどの記録媒体、104はチューナと復調器から構成されるレシーバ・デモジュレータ、105はMPEGデコーダ、106はMPEGトランスポートデコーダ、107は限定受信を行うためのセキュリティモジュール、108はセキュリティモジュール内で限定受信管理を行うICカード、109はスクランブルを解除するためのデスクランブラ、110はスクランブルを解除するために必要な鍵を含んだ情報である前記ECMおよびEMMをMPEGトランスポートストリームから選択するためのECM・EMMフィルタ、111はMPEGトランスポートストリーム入力切換回路、112はICカード108内にあるECM記憶領域、113はICカード108内にあるEMM記憶領域である。なおEMMはEMMを特定するための中間鍵ID情報であるEMM-IDが割り付けられてリスト形式で記憶されている。114はマスタ鍵Kmの記憶領域である。また図示していないが装置を特定するための装置ID情報もICカード108に記憶されている。

【0053】本実施形態ではEMMは衛星波に多重化されて送られてくる。まずスマートカード108にはあらかじめ装置ID情報とマスタ鍵Kmが記憶されている。EMMは1か月に一度更新され、衛星波に多重化されて送信されるが、この際EMMは装置ID情報を伴って送信される。レシーバ・デモジュレータ104により受信されたデータはMPEGトランスポートストリーム入力切換回路111に送られる。MPEGトランスポートストリーム入力切換回路111はECM・EMMフィルタ110にデータを転送し、ECM・EMMフィルタ110はデータからEMMおよび装置ID情報をフィルタリングして抽出し、ICカード108に送る。ICカード108は送られてきた装置ID情報と保持している装置ID情報を比較し、一致すればEMMをEMM記憶領域113に書き込み、一致しなければデータを破棄する。一致してEMMを書き込む際には、EMM-IDを割り付けてEMMとセットにしてEMM記憶領域113に格

納する。ここで EMM は 1 か月に一度更新されるものとするが、EMM の記録にあたっては更新前のデータに上書きせず、来歴記録としてリスト形式で保存される。

【0054】次にデジタル衛星放送の番組の記録について述べる。上記の EMM の記憶方法で述べた通り、EMM は抽出され、ECM・番組データと分離されている。ECM・番組データは ECM・EMM フィルタによりフィルタリングされた後、記録手段たる番組記録装置 102 により記録される。番組記録装置 102 はデジタルビデオとし、その記録媒体 103 は磁気テープとする。その記録の際、ECM・番組データの記憶領域のヘッダ領域に、EMM に対応付けられている EMM-ID を記録する。

【0055】次に記録番組データの再生について図 2 を使って説明する。図 2 の装置構成は図 1 に示した 101 のセットトップボックスから 114 のマスタ鍵 Km 記憶領域まで同様である。再生したい番組データが記録されている記録媒体 103 を番組記録装置 102 にセットして再生する。番組記録装置 102 は記録媒体 103 からデータを読み出し、MPEG トラストストリーム入力切替回路 111 に送る。MPEG トラストストリーム入力切替回路 111 は ECM・EMM フィルタ 110 にデータを転送制御し、ECM・EMM フィルタ 110 はデータから ECM およびヘッダにある EMM-ID をフィルタリングして抽出し、IC カード 108 に送り、残りの番組データをデスクランブラ 109 に送る。スマートカード 108 は ECM・EMM フィルタ 110 から送られてきた ECM を ECM 記憶領域 112 に記憶する。IC カード 108 は、さらに送られてきた EMM-ID を手掛かりに、EMM 記憶領域 113 中の EMM リストから一致する EMM-ID が割り付けられている EMM を選択する。次に、IC カード 108 は選択された EMM をマスタ鍵 Km により復号し、中間鍵たるワーク鍵 Kw を得る。さらに ECM をワーク鍵 Kw により復号し、スクランブル鍵 Ks を得て、得られた Ks をデスクランブラ 109 に送る。デスクランブラ 109 は番組データを Ks により復号し、スクランブルが解除されたデータを MPEG トラストストリームデコーダ 106 に送る。データは最終的に MPEG デコーダ 105 により MPEG 解凍され、モニタに映像データとして送られる。

【0056】以上により、記録媒体 103 に記録された番組データを長期間経過後、EMM が更新された後においても再生・視聴することができる。

【0057】なお、上記実施形態では番組記憶装置 102 は構成上、別筐体のビデオとしたが、内蔵されたものであってもよい。また記録媒体 103 として磁気テープとしたが、光磁気ディスク、CD-R（追記型 CD）、フォト CD、DVD（デジタルビデオディスク）、メモリカードなど可搬性のある記録媒体であればよく、また

は可搬性がない記録媒体である内蔵もしくは外付のハード磁気ディスク装置、メモリなどの記録媒体であってもよい。

【0058】また、EMM の更新期間を 1 か月としたが、運用により、別の周期で更新してもよい。例えば 1 週間に一度、番組ごとに 1 度であってもよい。

【0059】また、EMM と EMM-ID の記録する際のデータ構造をリスト形式としたが、両者を対応付けて、過去の来歴を残せる限り、データの構造はリスト形式に限らなくともよい。

【0060】また、EMM の送信は更新される度に 1 度衛星波による送信としたが、現行の EMM が有効な期間においても複数回送信されるものであってもよい。

【0061】（実施の形態 2）実施形態 2 を図 3 を使って説明する。実施形態 2 はデジタル衛星放送の番組を記録したデータを後日、あらかじめ設定されている他の装置においても視聴ができる例である。実施形態 1 と同様、長期間が経過してもスクランブルを解除し視聴することを可能とする。実施形態 1 は EMM が衛星波に多重化されて送られるものであったが、本実施形態では EMM の送信形態として電話回線を介した送信の例を挙げる。

【0062】図 3 において、104 は電話回線からデータを受信するモデムであるレシーバ・デモジュレータ、313 は他のデジタル放送受信装置に対応する EMM を記憶する第 2 EMM 記憶領域である。その他の構成 101 のセットトップボックスから 114 のマスタ鍵 Km 記憶領域までは実施形態 1 に示したものと同様であり、説明を省略する。

【0063】IC カード 108 にはあらかじめマスタ鍵 Km、装置 ID 情報および相互利用が設定されている他の装置の装置 ID 情報が記憶されている。EMM は 1 か月に一度更新され、装置 ID 情報を伴って電話回線により送信される。レシーバ・デモジュレータ 104 により受信されたデータは MPEG トラストストリーム入力切替回路 111 に送られる。MPEG トラストストリーム入力切替回路 111 は ECM・EMM フィルタ 110 にデータを転送し、ECM・EMM フィルタ 110 は EMM をフィルタリングして抽出し、IC カード 108 に送る。IC カード 108 は送られてきた EMM に伴っている装置 ID 情報を IC カード 108 内にある自らの装置 ID 情報と比較し、一致する場合は EMM 記憶領域 113 に追記記憶する。一致しない場合は設定されている他の装置 ID 情報と比較し、ここで一致する場合は第 2 EMM 記憶領域 313 に追記記憶する。EMM を書き込む際には実施形態 1 同様、EMM に EMM-ID を割り付けて、EMM と対応する EMM-ID のセットとして格納・保持する。その際に更新前の情報には上書きせずに来歴記録として残しリスト形式で保持する。

【0064】次にデジタル衛星放送の番組の記録について述べる。ECM・番組データはECM・EMMフィルタ110によりフィルタリングされた後、ECM・番組データ記録手段たる番組記録装置102に送られ、記録される。その際、現行のEMMをEMM記憶領域113から番組記憶装置102に伝達し、また現行の他の装置でのEMMを第2EMM記憶領域313から番組記憶装置102に伝達し、番組データのヘッダとして番組データとともに記憶する。番組記録装置102はデジタルビデオとし、その記録媒体103は磁気テープとする。その記録の際、ECM・番組データの記憶領域のヘッダ領域に、それぞれのEMMに対応付けられているEMM-IDも記録する。

【0065】次に番組データを記録した装置以外の他の装置での記録番組データの再生について図4を使って説明する。図4の装置構成は図1に示した101のセットトップボックスから114のマスタ鍵Km記憶領域まで同様である。なお、装置にある装置ID情報を装置ID情報2とし、記録した装置の装置ID情報を装置ID情報2とする。まず再生したい番組データが記録されている記録媒体103を番組記録装置102にセットして再生する。番組記録装置102は記録媒体103からデータを読み出し、MPEGトランスポートストリーム入力切替回路111に送る。MPEGトランスポートストリーム入力切替回路111はECM・EMMフィルタ110にデータを転送制御し、ECM・EMMフィルタ110はデータからECMおよびヘッダにあるEMM-IDと装置ID情報をフィルタリングして抽出し、ICカード108に送り、残りの番組データをデスクランブラ109に送る。ICカード108はECM・EMMフィルタ110から送られてきたECMをECM記憶領域112に記憶する。ICカード108は、さらに送られてきたおよびEMM-IDを手掛かりとしてEMM記憶領域113中のEMMリストから一致する装置ID情報およびEMM-IDが割り付けられているEMMを選択する。次にICカード108は選択されたEMMをマスタ鍵Kmにより復号し、中間鍵たるワーク鍵Kwを得る。さらにECMをワーク鍵Kwにより復号し、スクランブル鍵Ksを得て、得られたスクランブル鍵Ksをデスクランブラ109に送る。デスクランブラ109は番組データをKsにより復号し、スクランブルが解除されたデータをMPEGトランスポートデコーダ106に送る。データは最終的にMPEGデコーダ105によりMPEG解凍され、モニタに映像データとして送られる。

【0066】以上により、記録媒体103に記録された番組データを長期間経過後、EMMが更新された後、あらかじめ設定されている他の装置においても再生・視聴することができる。

【0067】本実施形態ではEMMの更新期間を1か月としたが、運用により、別の周期で更新してもよい。例

えば1週間に一度、番組ごとに1度であってもよい。

【0068】また、EMMと装置ID情報およびEMM-IDの記録する際のデータ構造をリスト形式としたが、両者を対応付けて、過去の来歴を残せる限り、データの構造はリスト形式に限らなくともよい。

【0069】また、EMMの送信は更新される度に1度電話回線による送信としたが、現行のEMMが有効な期間においても複数回送信されるものであってもよい。また実施形態1に示したように衛星波に多重化されて送信される場合も同様に考えることができる。

【0070】（実施形態3）実施形態3を図5を使って説明する。実施形態3も実施形態1または2と同様、デジタル衛星放送の番組を記録した後、長期間が経過してもスクランブルを解除し視聴することを可能とするデジタル衛星放送受信装置であり、共通鍵暗号方式を利用した3重鍵構造の限定受信方式による衛星放送システムを前提とする点も同様である。本実施形態ではEMM記憶領域が2つあり、図5において、113はEMM記憶領域の1つであり、513は他方のEMM記憶領域である。その他の構成は実施形態1に示したものと同一であり、構成の説明は省略する。本実施形態では実施形態1と同様、EMMは衛星波に多重化されて送信されるものとする。送信されるEMMは実施形態1と同様、装置ID情報を伴って送信される。レシーバ・デモジュレータ104により受信されたデータはMPEGトランスポートストリーム入力切替回路111に送られる。MPEGトランスポートストリーム入力切替回路111はECM・EMMフィルタ110にデータを転送し、ECM・EMMフィルタ110はデータからEMMおよび装置ID情報をフィルタリングして抽出し、ICカード108に送る。ICカード108は送られてきた装置ID情報と保持している装置ID情報を比較し、一致すればEMMをEMM記憶領域113および513両方に書き込み、一致しなければデータを破棄する。一致してEMMを書き込む際には、EMM-IDを割り付けてEMMとセットとしてEMM記憶領域113および513に格納する。ここでEMMは1か月に一度更新されるものとするが、前記EMMの記録にあたりEMM記憶領域113では更新前のデータに上書きし、常に現行のEMMを記憶する。一方EMM記憶領域513においては更新前のデータに上書きせず、過去のEMM情報およびEMM-IDを来歴記録としてリスト形式で保存する。

【0071】次に記録番組データの再生について図6を使って説明する。図6の装置構成は図5に示した101のセットトップボックスから114のマスタ鍵Km記憶領域まで同様である。まず再生したい番組データが記録されている記録媒体103を番組記録装置102にセットして再生する。番組記録装置102は記録媒体103からデータを読み出し、MPEGトランスポートストリーム入力切替回路111に送る。MPEGトランスポート

トストリーム入力切換回路111はECM・EMMフィルタ110にデータを転送制御し、ECM・EMMフィルタ110はデータからECMおよびヘッダにあるEMM-IDと装置ID情報をフィルタリングして抽出し、ICカード108に送り、残りの番組データをデスクランブラ109に送る。ICカード108はECM・EMMフィルタ110から送られてきたECMをECM記憶領域112に記憶する。ICカード108は、さらに送られてきたおおよびEMM-IDを手掛かりに、EMM記憶領域113および513中のEMMリストから一致する装置ID情報およびEMM-IDが割り付けられているEMMを選択する。EMM記憶領域513中のEMMリスト中に該当するEMMがある場合にはEMM記憶領域513からICカード108にそのEMMを送信する。次に、ICカード108は選択されたEMMをマスタ鍵Kmにより復号し、中間鍵たるワーク鍵Kwを得る。さらにECMをワーク鍵Kwにより復号し、スクランブル鍵Ksを得て、得られたスクランブル鍵Ksをデスクランブラ109に送る。デスクランブラ109は番組データをスクランブル鍵Ksにより復号し、スクランブルが解除されたデータをMPEGトランスポートデコーダ106に送る。データは最終的にMPEGデコーダ105によりMPEG解凍され、モニタに映像データとして送られる。

【0072】以上により、記録媒体103に記録された番組データを長期間経過後、EMMが更新された後、再生・視聴することができる。

【0073】なお、本実施形態では、EMM記憶領域513をビデオ装置内のメモリとしたが、セットトップボックス101内に記憶領域を設けてもよい。またECM・番組データ記憶媒体内にあってもよく、内蔵ハードディスク、大容量のメモリなどが挙げられる。またEMM記憶領域513を可搬性のある記憶媒体である磁気テープ、CD-R、DVDなどの記憶媒体に設けることも可能であり、その場合はEMM記憶領域513をECM・番組データ記憶領域のヘッダ領域に設ける構成がある。

【0074】（実施形態4）実施形態4を図7を使って説明する。実施形態4も実施形態1または2と同様、デジタル衛星放送の番組を記録した後、長期間が経過してもスクランブルを解除し視聴することを可能とするデジタル衛星放送受信装置であり、共通鍵暗号方式を利用した3重鍵構造の限定受信方式による衛星放送システムを前提とする点も同様である。また図7において、装置の構成101のセットトップボックスから114のマスタ鍵Km記憶領域までは実施形態1または2に示したものと同様であり、ここでは説明を省略する。さらにEMMの記憶において実施形態1または2におけるEMMの記憶と同様でよく、EMMの更新も実施形態1または2と同様に月に1度とする。ただし、本実施形態ではEMM-IDは必ずしも必要ではなく、EMM記憶領域113

には現行のEMMのみが記憶されている。

【0075】次にデジタル衛星放送の番組の記録について述べる。レシーバ・デモジュレータ104に受信された衛星波のデータはECM・EMMフィルタ110によりフィルタリングされた後、記録手段たる番組記録装置102により記録される。番組記録装置102はデジタルビデオとし、その記録媒体103は磁気テープとする。その記録の際、EMM記憶領域113に記憶されているEMMが前記番組記録装置102に伝達され、番組記録装置102は、ECM・番組データの記憶領域のヘッダ領域に、伝達されたEMMを記録する。このように記録媒体103にはECM・番組データとそれに対応するEMMがセットで記録され、EMMが後に更新され、EMM記憶領域113に記憶されている現行EMMが変わった場合でも番組データの再生に必要なEMMは失われない。

【0076】次に記録番組データの再生について図8を使って説明する。図8の装置構成は図7に示した101のセットトップボックスから114のマスタ鍵Km記憶領域まで同様である。再生したい番組データが記録されている記録媒体103を番組記録装置102にセットして再生する。番組記録装置102は記録媒体103からデータを読み出し、MPEGトランスポートストリーム入力切換回路111に送る。MPEGトランスポートストリーム入力切換回路111はECM・EMMフィルタ110にデータを転送制御し、ECM・EMMフィルタ110はデータからEMMおよびECMをフィルタリングして抽出し、ICカード108に送り、残りの番組データをデスクランブラ109に送る。ICカード108はECM・EMMフィルタ110から送られてきたECMをECM記憶領域112に記憶し、EMMをEMM記憶領域113に記憶する。この際、データ再生の前にEMM記憶領域113に格納されていた現行のEMMを上書きせずに一時的に退避させ、データ再生のために取り込んだEMMを再生用の一時利用のEMMとして使用する。次に、ICカード108は前記再生用EMMをマスタ鍵Kmにより復号し、中間鍵たるワーク鍵Kwを得る。さらにECMをワーク鍵Kwにより復号し、スクランブル鍵Ksを得て、得られたKsをデスクランブラ109に送る。デスクランブラ109は番組データをKsにより復号し、スクランブルが解除されたデータをMPEGトランスポートデコーダ106に送る。データは最終的にMPEGデコーダ105によりMPEG解凍され、モニタに映像データとして送られる。

【0077】以上により、記録媒体103に記録された番組データを長期間経過後、EMMが更新された後においても再生・視聴することができる。

【0078】なお、上記実施形態では番組記憶装置102は構成上、別筐体のビデオとしたが、内蔵されたものであってもよい。また記録媒体103として磁気テープ

としたが、光磁気ディスク、CD-R（追記型CD）、フォトCD、DVD、メモリカードなど可搬性のある記録媒体であればよく、または可搬性がない記録媒体である内蔵もしくは外付のハード磁気ディスク装置、メモリなどの記録媒体であってもよい。

【0079】また、EMMの更新期間を1か月としたが、運用により、別の周期で更新してもよい。例えば1週間に一度、番組ごとに1度であってもよい。

【0080】また、EMMの送信は更新される度に1度衛星波による送信としたが、現行のEMMが有効な期間においても複数回送信されるものであってもよい。

【0081】

【発明の効果】以上のように本発明によれば番組を記録した後、長期間が経過してEMMが更新された場合でも、記録番組データのスクランブルを解除し、視聴が可能となり、また記録に用いたデジタル放送受信装置とは異なる他のデジタル衛星放送受信装置で再生した場合でも同様に記録番組データのスクランブルを解除し、視聴することが可能となる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るデジタル放送受信装置の構成図

【図2】本発明の第1の実施形態に係るデジタル放送受信装置の構成図

【図3】本発明の第2の実施形態に係るデジタル放送受信装置の構成図

【図4】本発明の第2の実施形態に係るデジタル放送受信装置の構成図

【図5】本発明の第3の実施形態に係るデジタル放送受

信装置の構成図

【図6】本発明の第3の実施形態におけるデジタル放送受信装置の構成図

【図7】本発明の第4の実施形態におけるデジタル放送受信装置の構成図

【図8】本発明の第4の実施形態におけるデジタル放送受信装置の構成図

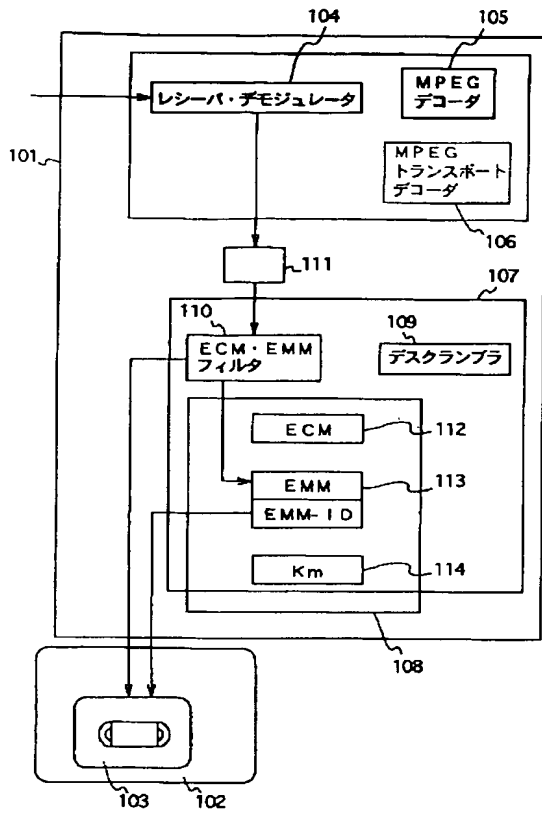
【図9】従来の技術によるデジタル放送受信装置の構成図

10 【図10】従来の技術によるデジタル放送受信装置の構成図

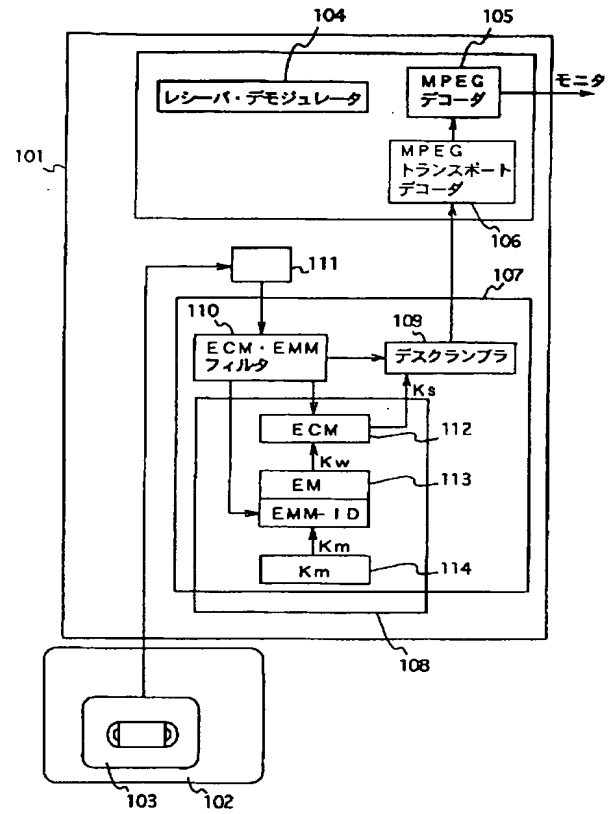
【符号の説明】

101, 901 デジタル放送受信装置
102, 902 番組記録装置
103, 903 記録媒体
104, 904 レシーバ・デモジュレータ
105, 905 MPEGデコーダ
106, 906 MPEGトランスポートデコーダ
107, 907 セキュリティーモジュール
20 108, 908 ICカード
109, 909 デスクランブラ
110, 910 ECM・EMMフィルタ
111, 911 MPEGトランスポートストリーム入力切替回路
112, 912 ECM記憶領域
113, 513, 913 EMM記憶領域
114, 914 マスタ鍵Km記憶領域
313 第2EMM記憶領域

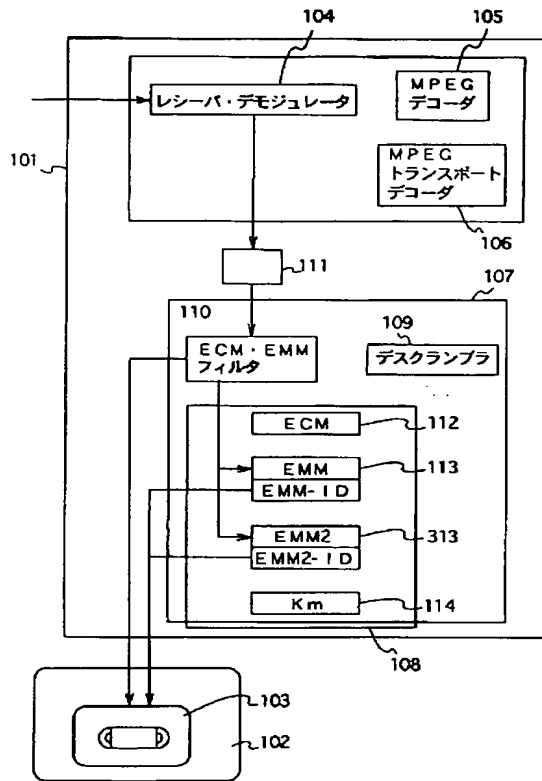
【図1】



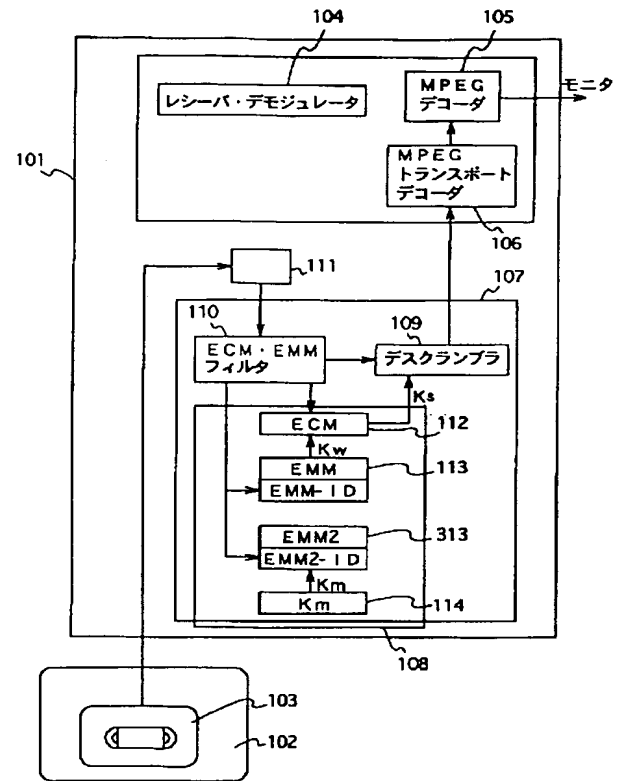
【図2】



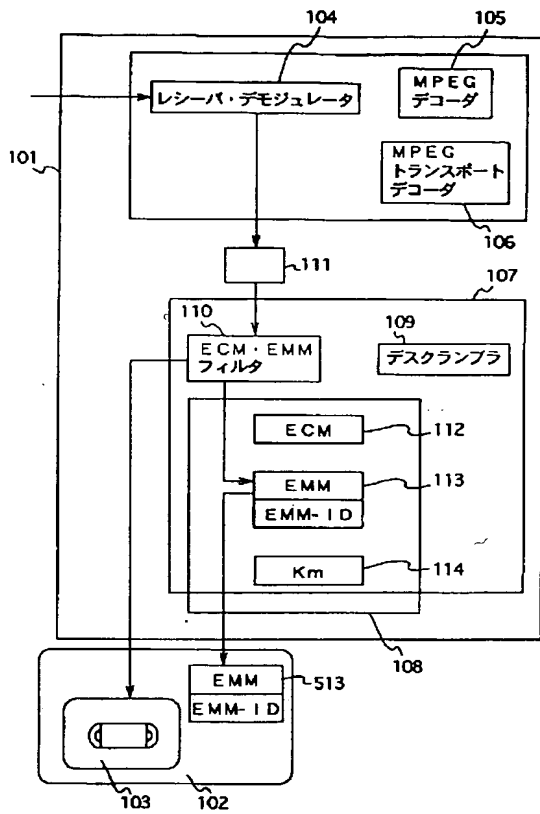
【図3】



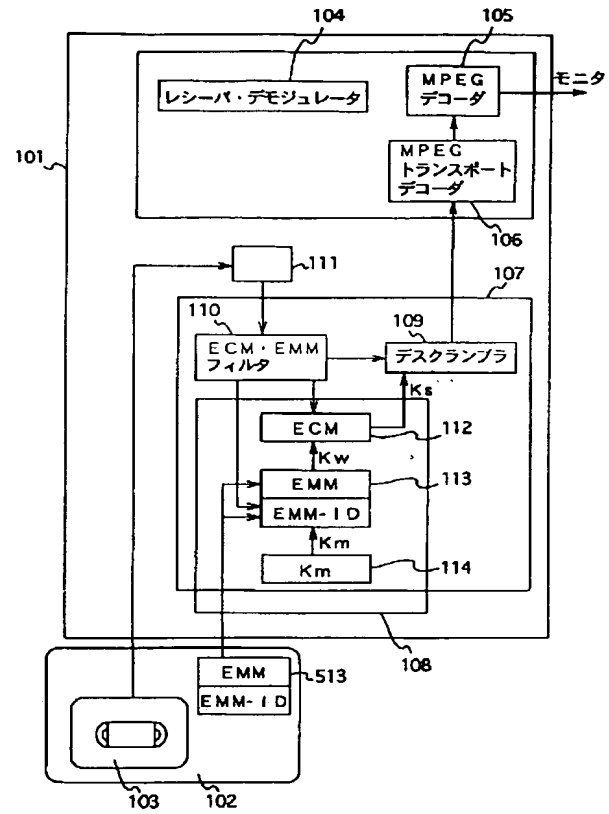
【図4】



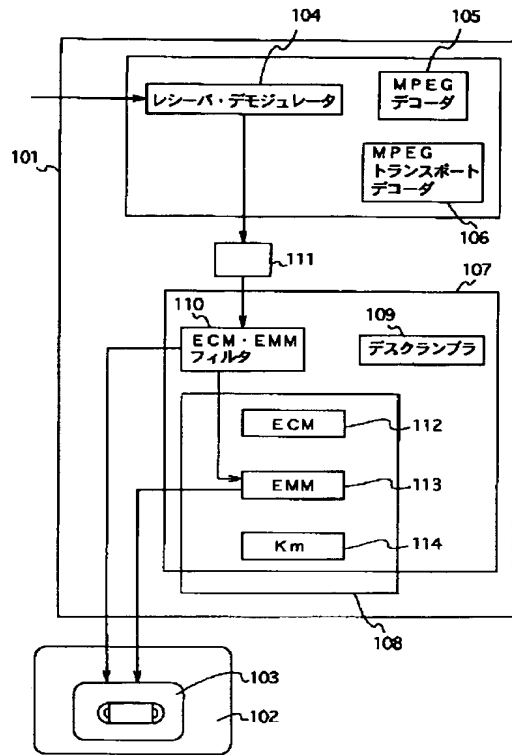
【図5】



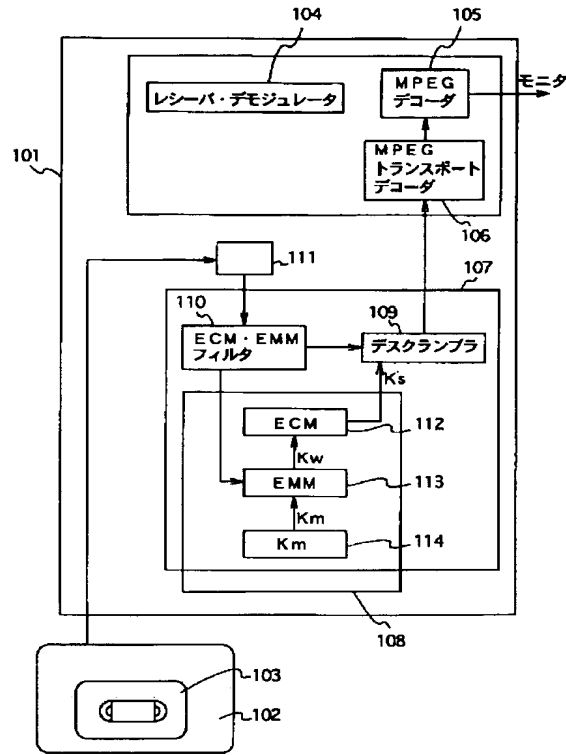
【図6】



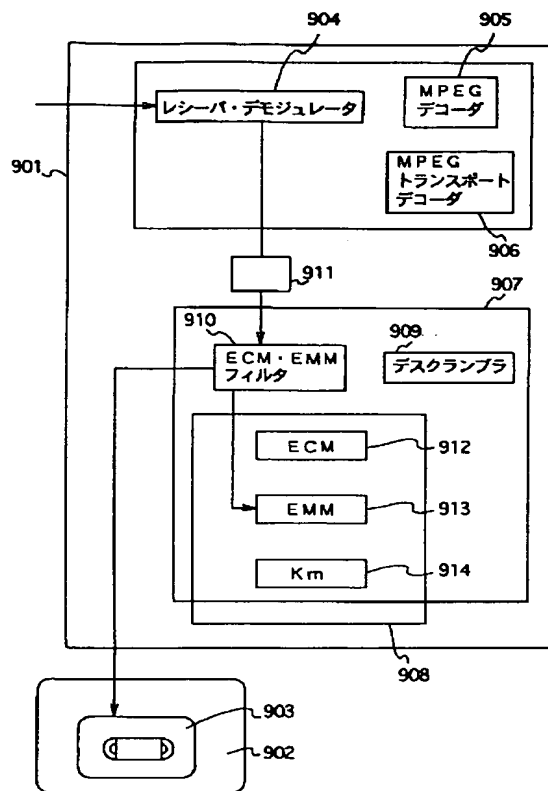
【図7】



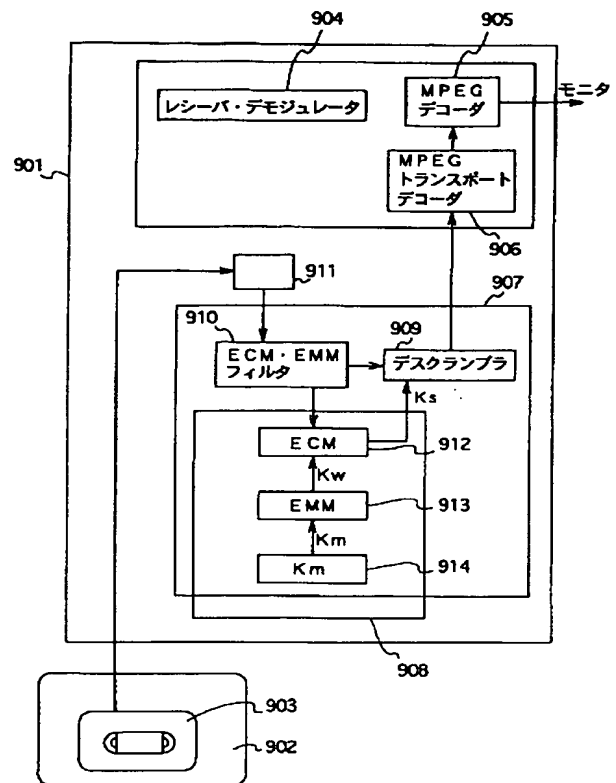
【図8】



【図9】



【図10】



フロントページの続き

(51) Int. Cl.⁶

H04N 5/91

識別記号

F I

H04N 5/91

Z